

Interagency Advisory Board

Meeting Agenda, Wednesday, June 29, 2011

1. **Opening Remarks** (*Mr. Tim Baldrige, IAB Chair*)
2. **Using PKI to Mitigate Leaky Documents** (*John Landwehr, Adobe*)
3. **The Digital Identity Ecosystem of the States: Leveraging Federal Initiatives** (*Doug Robinson, NASCIO*)
4. **Achieving Federal Identity Compliance in PACS Without a Rip-and-Replace Investment** (*Dave Adams, HID*)
5. **Aviation Credentialing and the New RTCA Standard 230C** (*Christer Wilkerson, AECOM*)
6. **Closing Remarks** (*Mr. Tim Baldrige, IAB Chair*)



PKI Protection for Leaky Documents

June 2011 | John T. Landwehr | Sr. Director, Enterprise Security Solutions



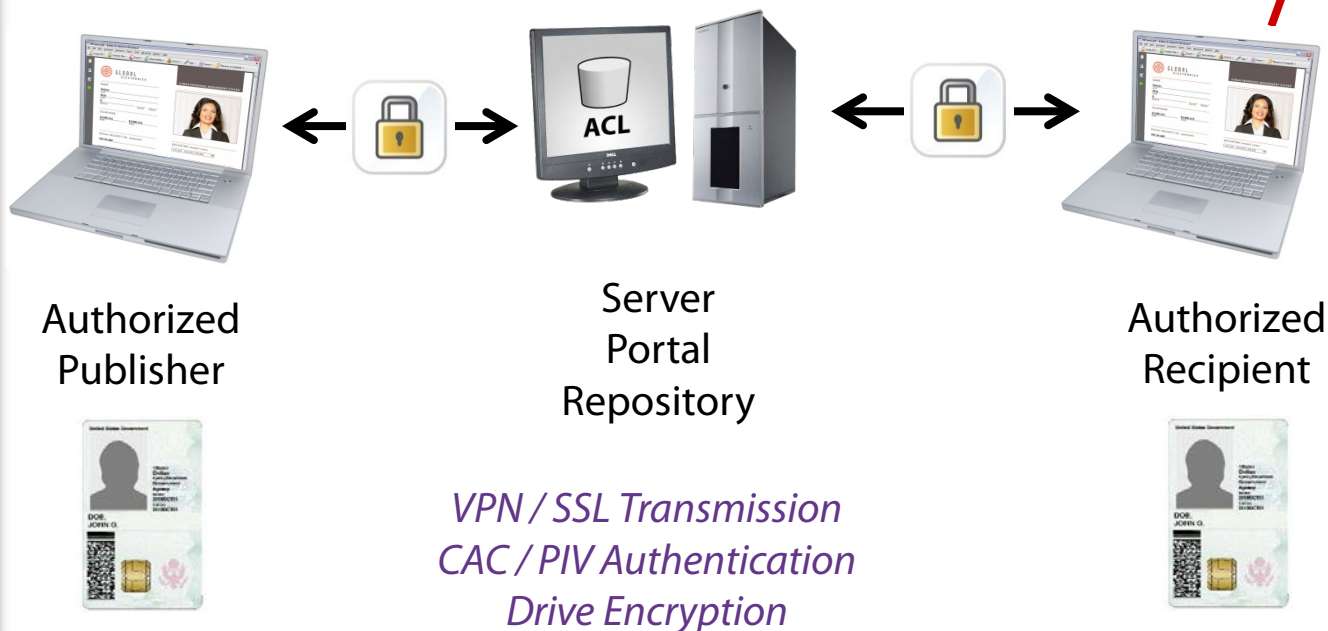
Information Sharing Challenges

Redistribution without security!



When sensitive documents leave protected storage and networks, it has been difficult to maintain:

Authenticity
Integrity
Confidentiality
Privacy





Two-factor Authentication

CAC Pin:

PIN required. 3 tries remaining

DCO DEFENSE CONNECT ONLINE

Login



Digital Signatures

This document was certified by Superintendent of Documents <pkisupport@gpo.gov>, United States Government Printing Office with a valid certificate issued by GeoTrust CA for Adobe.

Signature Properties

information, or any other return reason.

27. SIGNATURE Digitally signed by John Landwehr Date: 2008.03.07 10:00:18 -08'00'

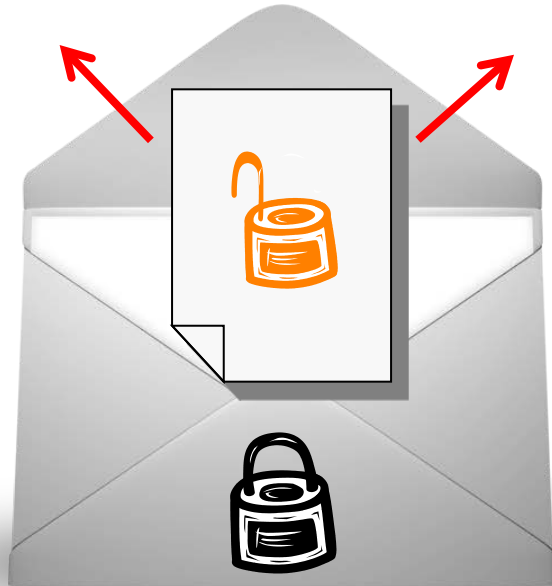


Content Encryption



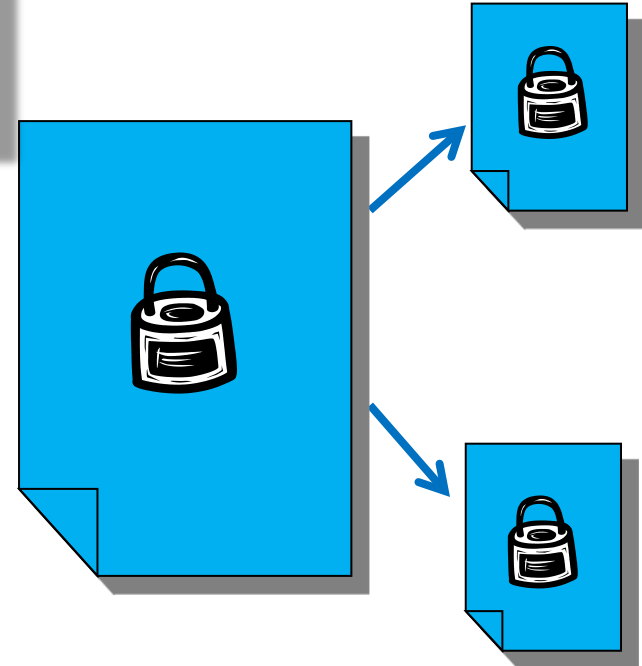
PKI for content encryption has been challenging to effectively implement and use

Protecting the container vs. *the content*



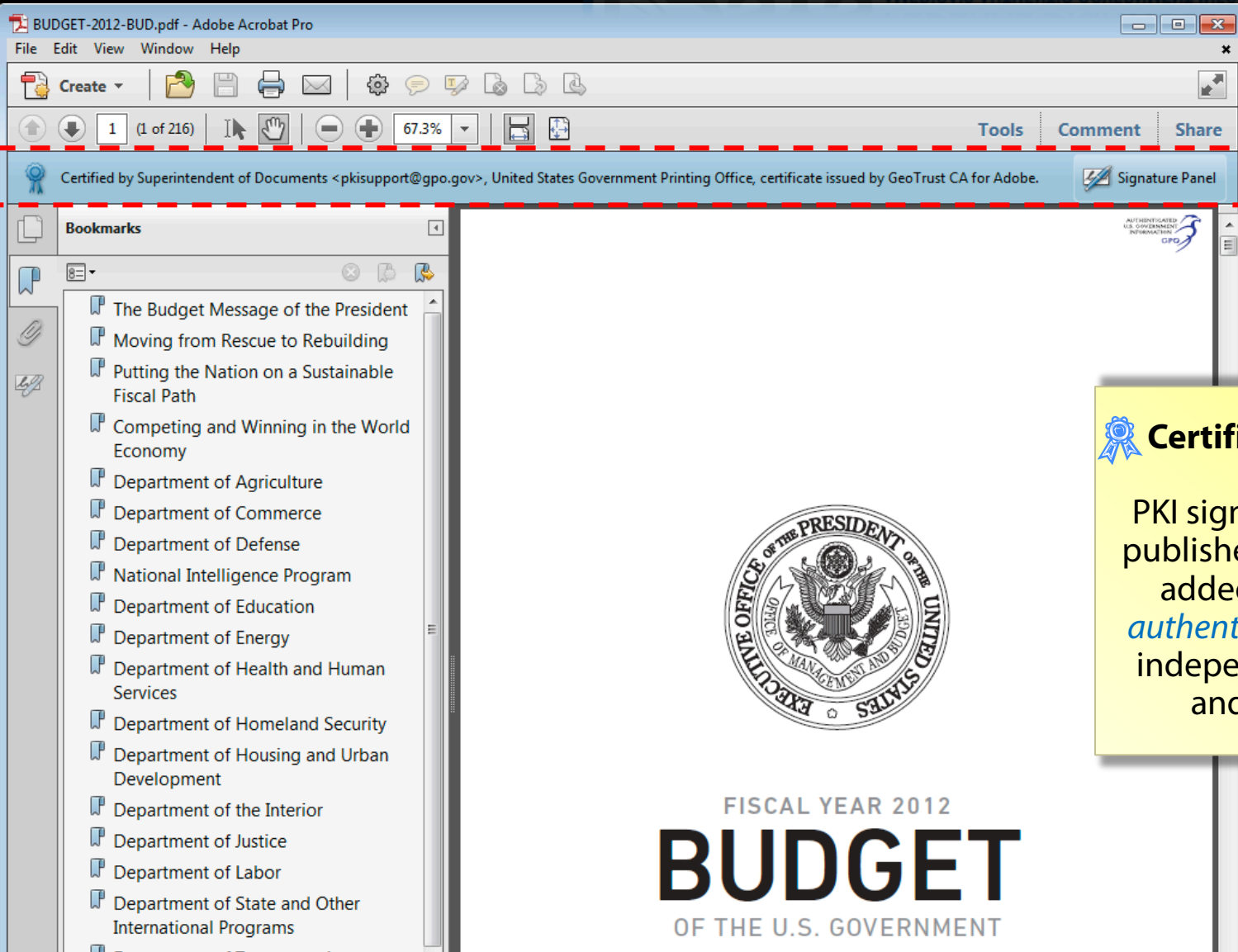
With traditional enveloped encryption, like S/MIME, PGP, or ZIP, the container is decrypted to produce the contents. You can't protect where the decrypted contents subsequently go.

*Certified
Documents
&
Rights
Management*



With internal document cryptography, there are no unprotected copies. The encryption is inside the file format itself. Wherever the document goes, it stays protected.

www.gpo.gov



Certified Documents

PKI signature applied by publisher gives recipients added assurances of *authenticity and integrity*, independent of storage and distribution

Certified Transcripts (digitally signed PDFs)

Schools are using PKI to persistently protect the authenticity, integrity, and privacy of electronic student transcripts



Cornell University



NC STATE UNIVERSITY

NORTHWESTERN
UNIVERSITY



STANFORD
UNIVERSITY

UNIVERSITY OF
MINNESOTA



Reference: <http://www.avowsystems.com/clients.php>



Not only can PKI
signatures be persistent
and stick to the content –

Encryption can too.

And work together





VERIFIED OFFICIAL STANFORD TRANSCRIPT IN PDF FORMAT ONLY



STANFORD UNIVERSITY

OFFICE OF THE UNIVERSITY REGISTRAR

STANFORD, CA 94305-6032

Name: Wonka, Warren G.
Student ID: 09876543

Thomas C. Black
Thomas C. Black
University Registrar

In accordance with USC 438 (6) (4) (8) (The Family Educational Rights and Privacy Act of 1974), you are hereby notified that this information is provided upon the condition that you, your agents or employees will not permit any other party access to this record without consent of the student. Alteration of this transcript may be a criminal offense.

Print Date : 29 Oct 2007

-----Academic Program-----

Program : Undergraduate Matriculated
25 Sep 2006 : Undeclared Undergraduate Major
Active in Program

-----Transfer Credit-----

Applied Toward Undergraduate Matriculated Program
Transfer Credit from University of California, Riverside
Quarter Units Posted: 6.00
Total Quarter Units Posted: 6.00
Allowable AP/transfer credit subject to restrictions.

-----Advanced Placement Test Credit-----

Applied Toward Undergraduate Matriculated Program
2006-2007 Autumn
Advanced Placement Chemistry 4.00
Advanced Placement Mathematics: Calculus AB 5.00
Total Quarter Units Posted: 9.00
Allowable AP/transfer credit subject to restrictions.

-----Beginning of Academic Record-----

2006-2007 Autumn

Subject	#	Title	Att	Ern	Grd
CHEM	31X	CHEMICAL PRINCIPLES	4.00	4.00	B-
		Boudart, M			
IHUM	63	FREEDOM, EQUALITY, DIFFERENCE	5.00	5.00	A
		Callan, E; Satz, D			
MATH	41	CALCULUS	6.00	6.00	B+
		Lucianovic, M			
ME	389	BIOENGINR & BIODESIGN FORUM	1.00	1.00	S
		Yock, P; Taylor, C			

2006-2007 Winter

Subject	#	Title	Att	Ern	Grd
CHEM	33	STRUCTURE AND REACTIVITY	4.00	4.00	C+
		Newton, A			
IHUM	27A	ENCOUNTERS AND IDENTITIES	5.00	5.00	A-
		Khan, K			
MATH	51A	LIN ALG AND MULTIVAR CALCULUS	6.00	6.00	B
		Newton, I			
SPANLANG	10	BEGINNING ORAL COMMUNICATION	2.00	2.00	S
		de Vega, L			

2006-2007 Spring

Subject	#	Title	Att	Ern	Grd
CHEM	35	ORG MONOFUNCTIONAL CMPDS	4.00	4.00	C-
		Spinoza, H			
CHEM	36	ORG CHEM LAB I	3.00	3.00	B-
		Darwin, C			
IHUM	27B	ENCOUNTERS AND IDENTITIES	5.00	5.00	B+
		Khan, K			
PWR	1	WRITING AND RHETORIC I	4.00	4.00	A
		Aristoteles, A			

-----End of Transcript-----



<

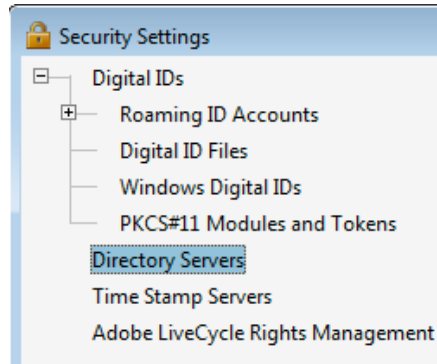
<

++

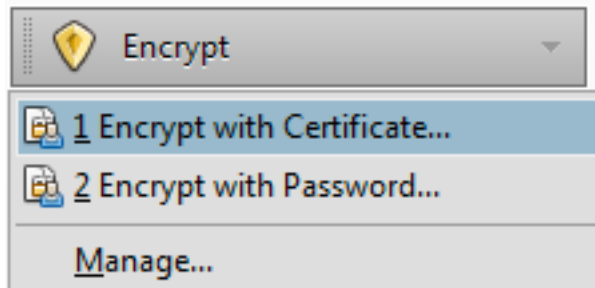
+1

Should you use PKI for persistent encryption? It is possible...

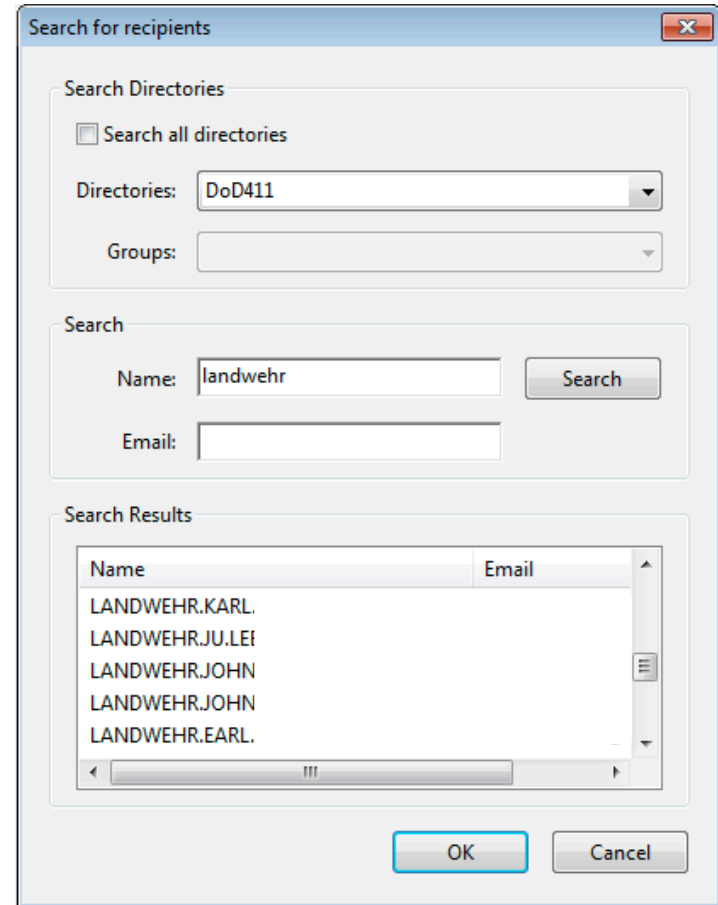
1. Configure an LDAP directory to look up public key certs



2. Specify certificate encryption



3. Search for recipients



PKI encrypting documents

- Document remains persistently protected
 - Independent of subsequent storage/transport
- Requires authorized CAC/PIV + PIN to open every time
 - Unauthorized users cannot view
- Can encrypt a single document instance to multiple recipients
 - The doc's symmetric key encrypted to each recipient's public key
- Each recipient can have different permissions
 - Print, modify, clipboard controls of protected content

Remaining challenges with only *standalone* PKI encryption of documents

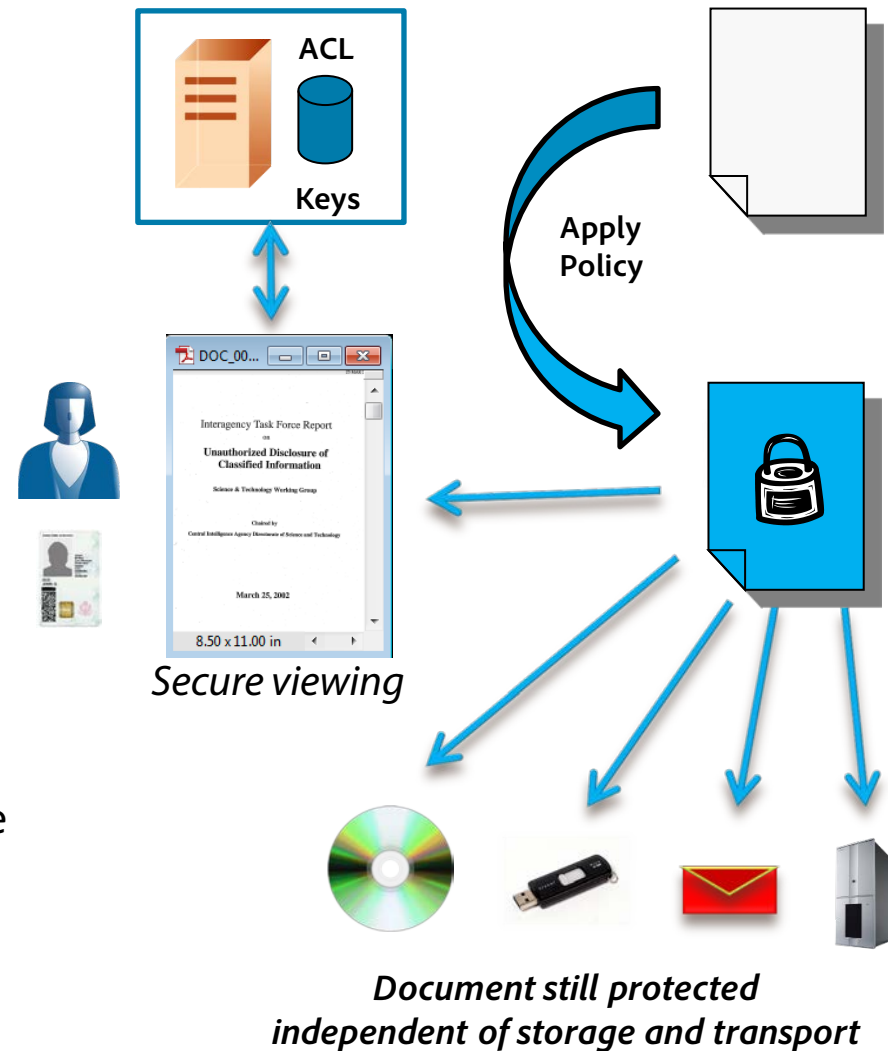
- Need to add more recipients? ... Republish
- Want to change the permissions? ... Republish
- Want to expire , revoke, or version control the document itself? ... N/A
- Want to audit who is accessing, or who is trying to access docs? ... N/A
- Want to dynamically watermark documents for printing? ... N/A
- Want to support multiple file types with one encryption system? ... N/A
- What about key management? ... Key management is required and critical
- Have a lot of authorized users? Especially with role based access? Or ties to a portal like SharePoint? Or a DLP systems? ... That's complicated!

Frustrated with
these limitations?
There is a solution!
(Rights Management)



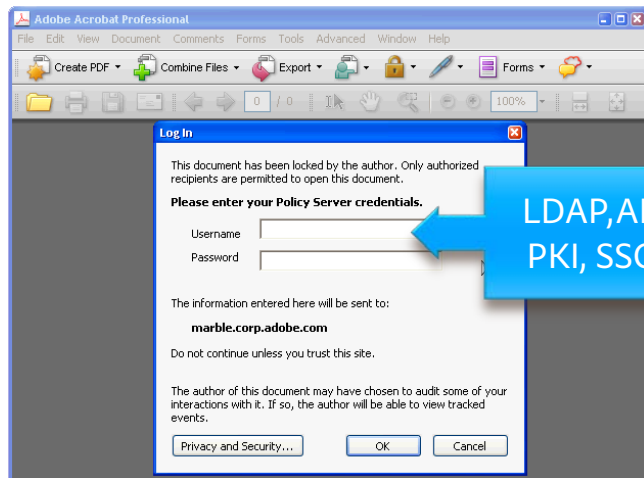
A better approach – Enterprise Rights Management

- User adds protection by picking an access “policy” from a key management server.
- The policy defines users and groups with *role based access* to content
- Document does not touch the key server; you still control where it is stored and how it is distributed.
- Resulting document is protected:
 - Always stays encrypted when distributed, even after authorized users open it.
 - Integrated with desktop apps for multiple file formats.
- Documents can be protected individually, in bulk, and via automated process, including DLP and portals.

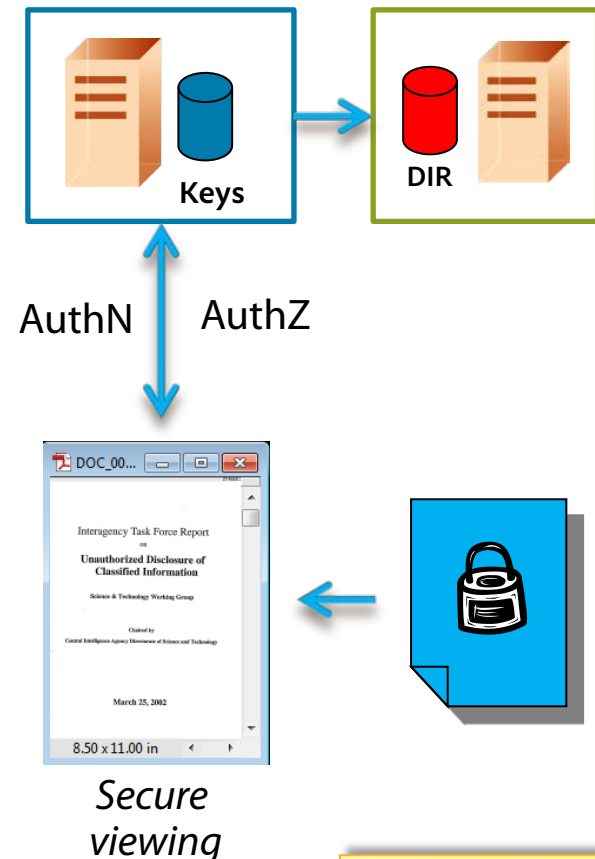


Rights Management with Enterprise Integration and PKI

- Server grants access to symmetric keys (AES256) after validating user identity and authorization.
- This can tie into existing enterprise systems like ActiveDirectory or LDAP, PKI certificates (e.g., CAC or PIV cards), or single sign-on.



LDAP, AD
PKI, SSO



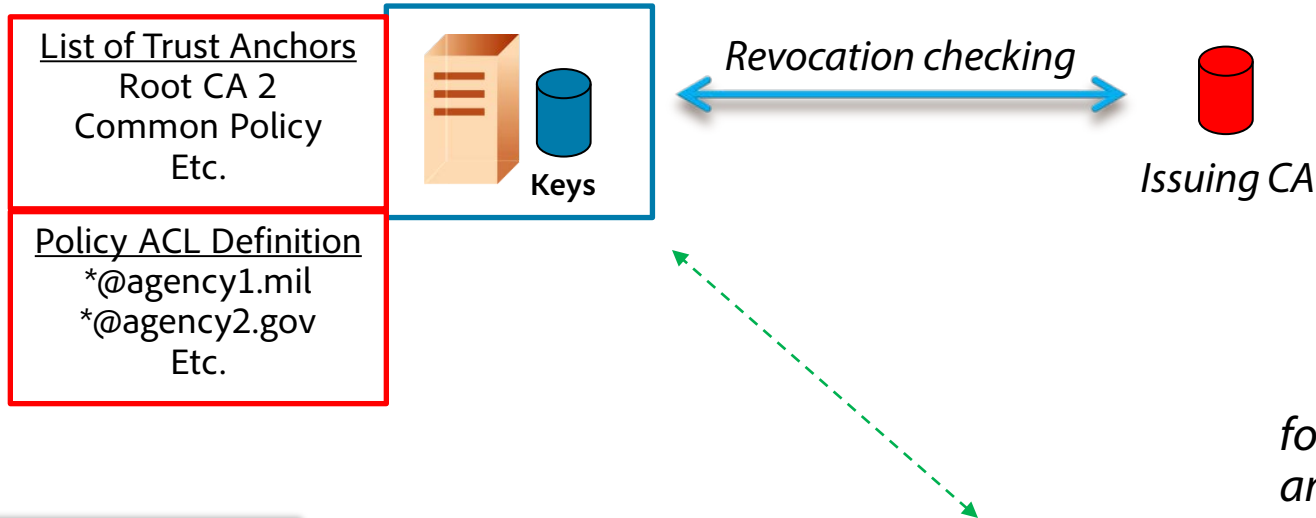
- Document protection can also be integrated into content repositories, e.g. SharePoint

Note:
PKI is
optional

Authenticating and authorizing external users with PKI

Publishing Organization

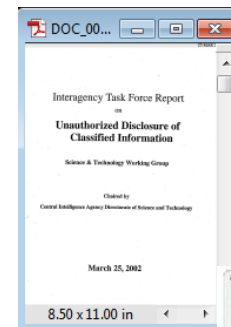
Recipient Organization



Federal PKI supports natural federation for authentication and authorization – providing more secure information sharing across agencies with rights management.



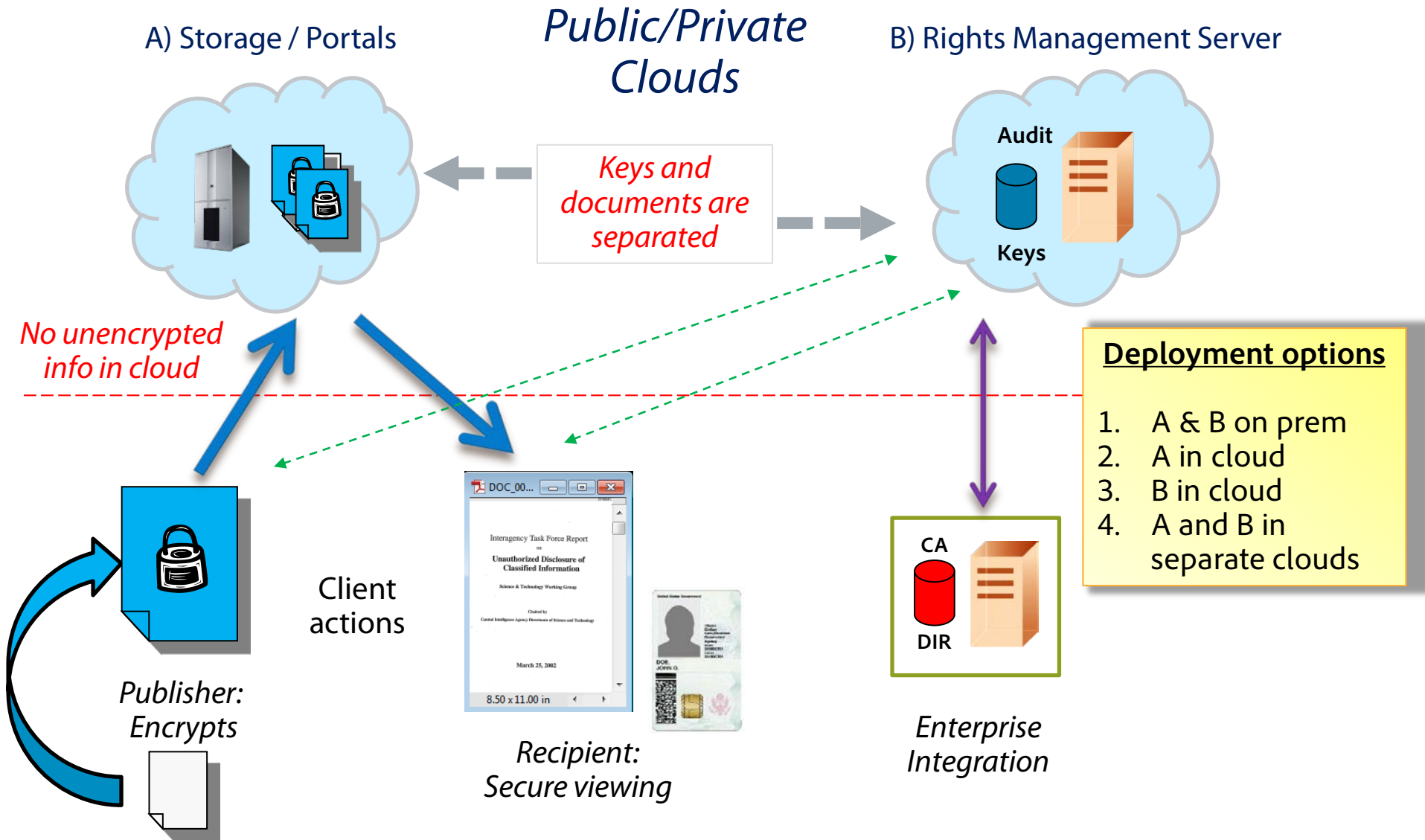
Information
Sharing
Portal



Secure
viewing

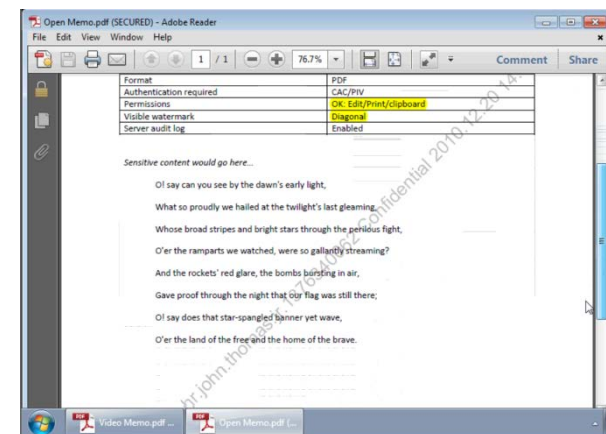
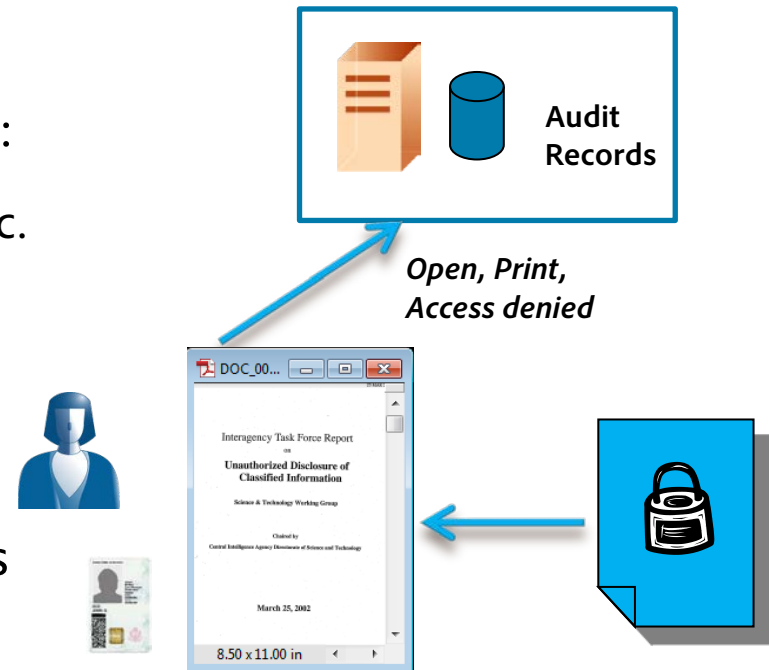


Securing data in the cloud



Continuous monitoring with detective controls

- Because access requests go through the server, it can provide additional functions:
 - Track (audit) access, printing, modifying, etc.
 - Limit functional access (e.g., printing)
 - Expiration or revocation of access
- These controls can change at any time, regardless of where protected documents live.
- Client provides:
 - Online and "Offline" access to documents
 - Add watermarks to the document



Detailed usage analytics – users and content



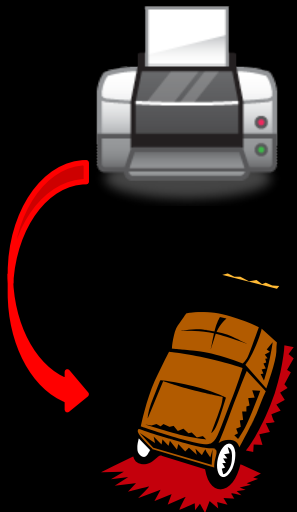
Continuous monitoring for usage anomalies

Discovering users who view and/or print unusual numbers of documents

Alert: User Mallory exceeds their average daily opens



User	Avg Opens	Today	Yesterday
Alice	15	17	12
Bob	23	24	23
Chris	7	7	6
Mallory	17	50	19



Alert: User Mallory exceeds their group's average daily prints

Group Avg	User	Prints Today	Yesterday
8	Alice	8	6
	Bob	12	14
	Chris	3	4
	Mallory	35	10

Sounds great, but how complicated is it to use?



**Author experience
(only two clicks!)**

Tools Comment Share

SENSITIVE INFORMATION

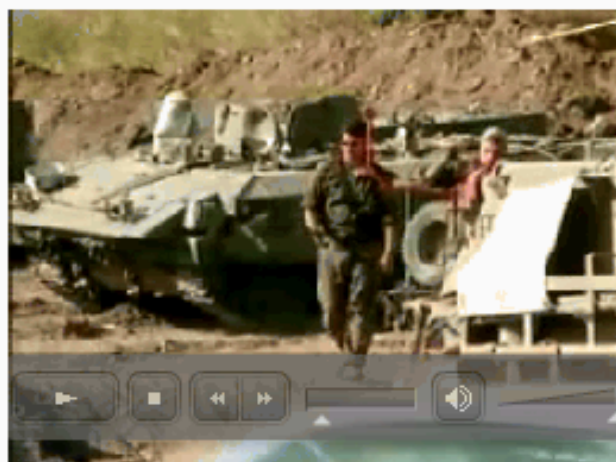
TO: ALL

FROM: HQ

This document utilizes rights management.

Capability	Detail for this document
Format	PDF with embedded Video
Authentication required	None / Anonymous
Permissions	Restricted: Edit/Print/clipboard
Visible watermark	Header
Server audit log	Enabled

Sensitive content would go here...



Pages
Content
Forms
Action Wizard
Recognize Text
Protection

Encrypt

- 1 MyPolicies:Public - View Only
- 2 MyPolicies:USG - Restricted Collaboration
- 3 MyPolicies:USG - View Only

Manage...

Remove

Apply Redactions
Redaction Properties
Search & Remove Text





Microsoft
Office Wo...



Microsoft
Office Exc...



Microsoft
Office Po...

Recipient experience



Adobe
Acrobat X Pro



Adobe Reader
X



Content -
Shortcut

Opening a protected document, restricted to
USG users with their smartcard badge.



Restricted
Memo.pdf



Open
Memo.pdf



Form.pdf



Video
Memo.pdf



Word DOC
Memo.docx



Revoked
Memo.pdf

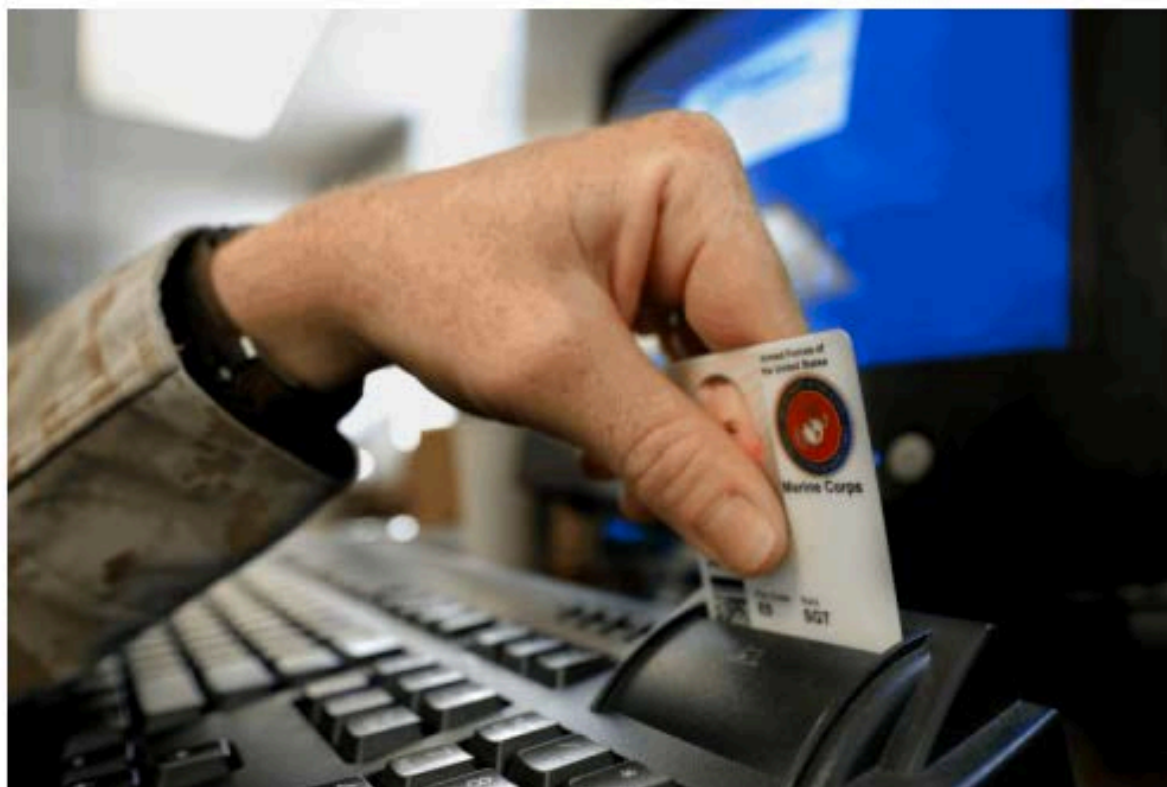


NoAccess
Memo.pdf



Video Memo.pdf ...

User inserts CAC/PIV badge into card reader





Adobe Reader



File Edit View Window Help



0 / 0



100%



Comment

Share



ADOBE®

Open a



Prote



Form



Open



Restr



VIDEOMEMO.pdf



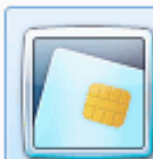
Open...

Windows Security



Microsoft Smart Card Provider

Please enter your PIN.



PIN

.....

[Click here for more information](#)

OK

Cancel



Video Memo.pdf ...



Adobe Reader



Windows Security



Security Settings



This document is secured using
"USG - View Only".



You cannot edit, print or copy
this document.

This document will not expire.

This document cannot be
opened offline.

[Permission Details](#)

SENSITIVE INFORMATION

In addition to restricting open
access with USG smartcard, this
document also restricts edit, print,
and clipboard operations

Server audit log	Enabled
------------------	---------

Sensitive content would go here...

O! say can you see by the dawn's early light,
What so proudly we hailed at the twilight's last gleaming,
Whose broad stripes and bright stars through the perilous fight,
O'er the ramparts we watched, were so gallantly streaming?
And the rockets' red glare, the bombs bursting in air,
Gave proof through the night that our flag was still there;
O! say does that star-spangled banner yet wave,
O'er the land of the free and the home of the brave.



Video Memo.pdf ...



Restricted Memo....

Adobe Reader

File Edit View Window Help



Comment

Share

***Accidentally or maliciously
received content,
but no access to view***



Error Information



You do not have access to this document. Contact John Landwehr for more information.

OK



Restricted Memo.pdf



ProtectedVideoMemo.pdf



Open...



demonstration.pd...



Adobe Reader



Security Settings



This document is secured using
"USG - View Only".



You cannot edit, print or copy
this document.



This document will not expire.

This document cannot be
opened offline.

[Permission Details](#)

Applies to forms, too

13 YOUR SPOUSE

Mark one box to show your current marital status and provide information about your spouse(s) in items a. and/or b.

☐ 1 - Never married
 ☐ 3 - Separated
 ☐ 5 - Divorced
☒ 2 - Married
 ☐ 4 - Legally Separated
 ☐ 6 - Widowed

a Current Spouse Complete the following about your current spouse only.

Full Name: Jane Doe
 Date of Birth: 07/04/1776
 Place of Birth (include country if outside the U.S.): Philadelphia, PA
 Social Security Number: 123-45-6789

Other Names Used (Specify maiden name, names by other marriages, etc., and show dates used for each name):
 Country(ies) of Citizenship: USA

Date Married:
 Place Married (include country if outside the U.S.):
 State:

If Separated, Date of Separation:
 If Legally Separated, Where is the Record Located? City (Country):
 State:

Address of Current Spouse, if different than your current address (Street, city, and country if outside the U.S.):
 State:
 ZIP Code:

b Former Spouse(s) Complete the following about your former spouse(s), use blank sheets if needed.

Full Name:
 Date of Birth:
 Place of Birth (include country if outside the U.S.):
 State:

Country(ies) of Citizenship:
 Date Married:
 Place Married (include country if outside the U.S.):
 State:

Check one, Then Give Date:
 Month/Day/Year:
 If Divorced, Where is the Record Located? City (Country):
 State:

☐ Divorced
 ☐ Widowed

Address of Former Spouse (Street, city, and country if outside the U.S.):
 State:
 ZIP Code:
 Telephone Number: () -

14 YOUR RELATIVES AND ASSOCIATES

Give the full name, correct code, and other requested information for each of your relatives and associates, living or dead, specified below.

1 - Mother (first)
 5 - Foster parent
 9 - Sister
 13 - Half-sister
 17 - Other Relative*
 2 - Father (second)
 6 - Child (adopted also)
 10 - Stepbrother
 14 - Father-in-law
 18 - Associate*
 3 - Stepmother
 7 - Stepchild
 11 - Stepsister
 15 - Mother-in-law
 19 - Adult Currently Living With You
 4 - Stepfather
 8 - Brother
 12 - Half-brother
 16 - Guardian

*Code 17 (Other Relative) - include only foreign national relatives not listed in 1 - 16 with whom you or your spouse are bound by affection, obligation, or close and continuing contact. Code 18 (Associate(s)) - include only foreign national associates with whom you or your spouse are bound by affection, obligation, or close and continuing contact.

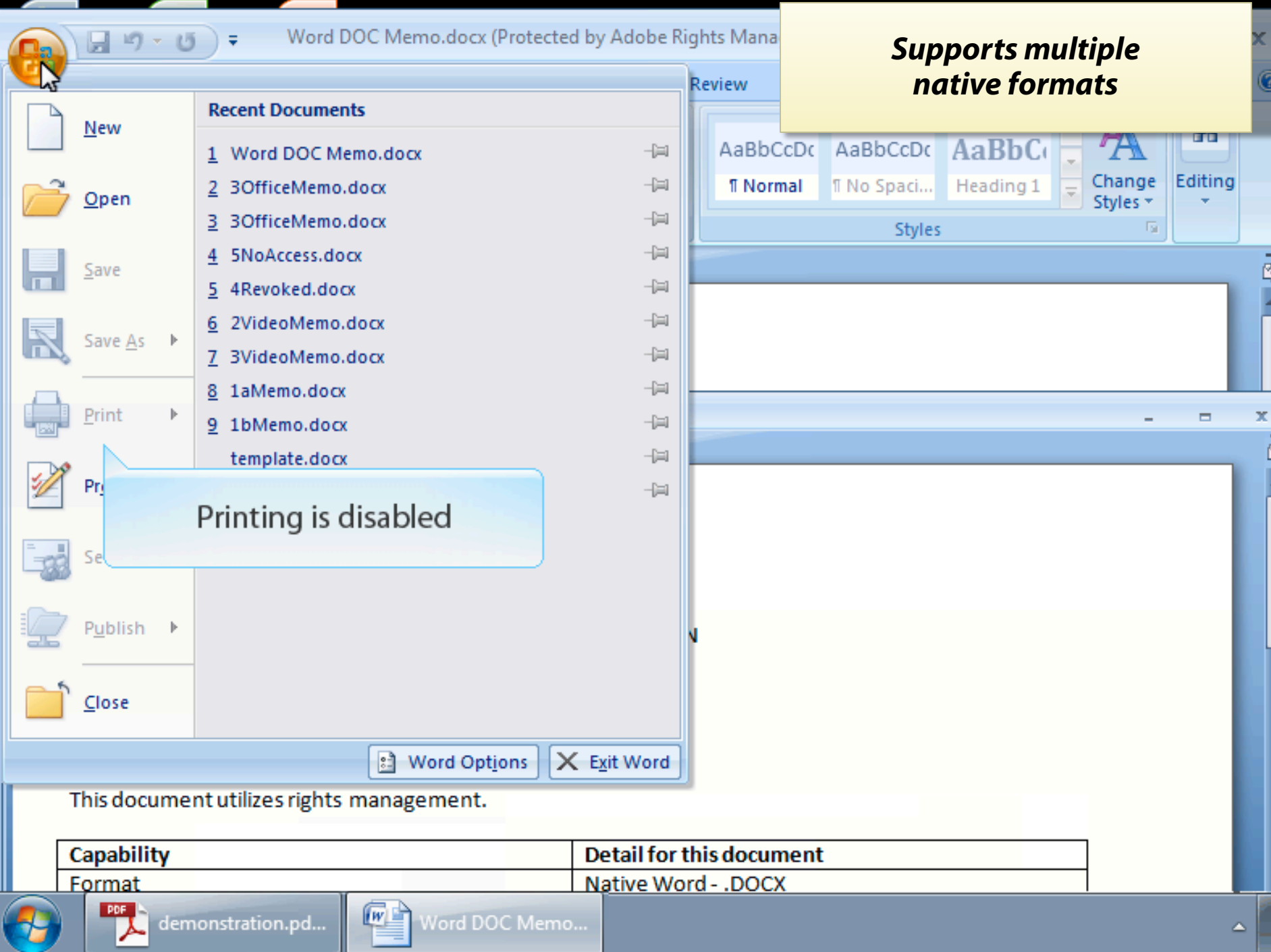
Full Name (If deceased, check box on the left before entering name)	Code	Date of Birth Month/Day/Year	Country of Birth	Country(ies) of Citizenship	Current Street Address and City (country) of Living Relatives	State
<input type="checkbox"/>	1					
<input type="checkbox"/>	2					
<input type="checkbox"/>						
<input type="checkbox"/>						



Video Memo.pdf ...



Form.pdf (SECUR...



Printing is disabled

***Supports multiple
native formats***

This document utilizes rights management.



















Capability



























Detail for this document

Format

Native Word - .DOCX

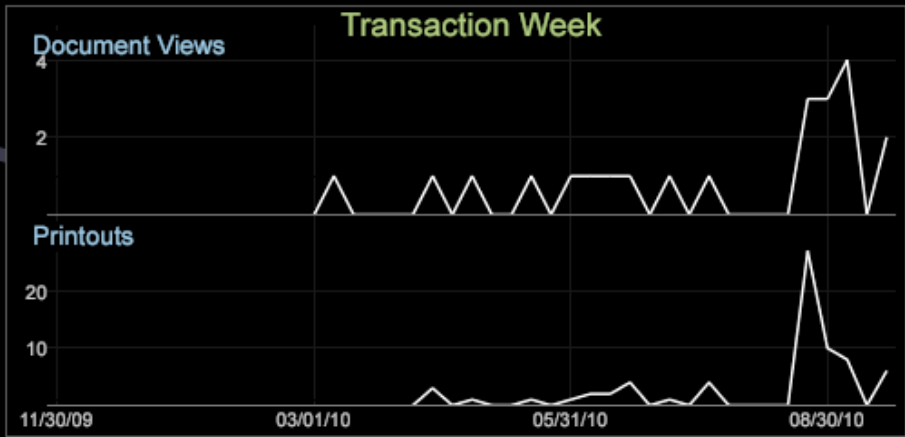
Employees Exceeding Document Printing Thresholds

Employee	Average Document Printouts	Current Printout Levels	Printout Alert Pct
Steve Higgins	17 	220 	1,192.2% 
Marc Eaman	28 	86 	208.4% 
Charles Hanflik	26 	56 	115.5% 
Barry Graham	65 	75 	15.2% 
David Liao	17 	14 	-17.4% 
Eiichi Kitagawa	12 	9 	-22.0% 

Documents	Document Views	Printouts
Project 003 - (01/05/2008) - draft v3.pdf	1 	2 
Project 122 - (03/19/2010) - draft v2.pdf	2 	14 
Project 125 - (03/21/2008) - draft v2.pdf	1 	2 
Project 192 - (07/12/2009) - draft v3.pdf	2 	2 
Project 201 - (04/11/2009) - draft v3.pdf	2 	8 
Project 512 - (02/24/2011) - final draft.pdf	22 	70 
Project 551 - (07/30/2008) - draft v2.pdf	1 	1 
Project 555 - (07/30/2008) - draft v2.pdf	1 	2 
Project 651 - (02/10/2010) - draft v1.pdf	1 	3 
Project 731 - (06/09/2010) - draft v3.pdf	2 	5 
Project 860 - (03/26/2011) - draft v2.pdf	1 	3 
Project 928 - (05/03/2009) - draft v4.pdf	1 	2 
Project 998 - (12/19/2010) - draft v2.pdf	1 	1 

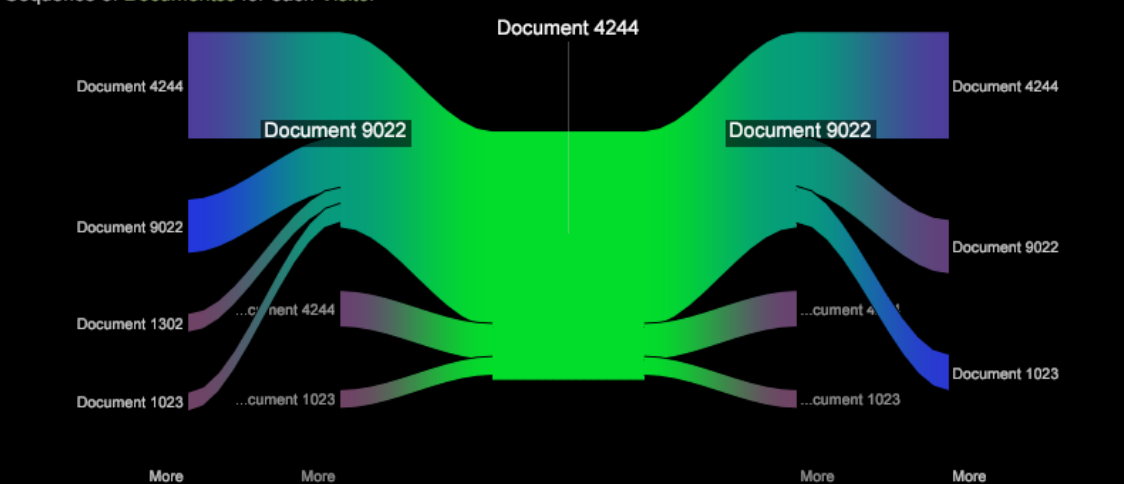
Trending Documents >>

<< Current Documents



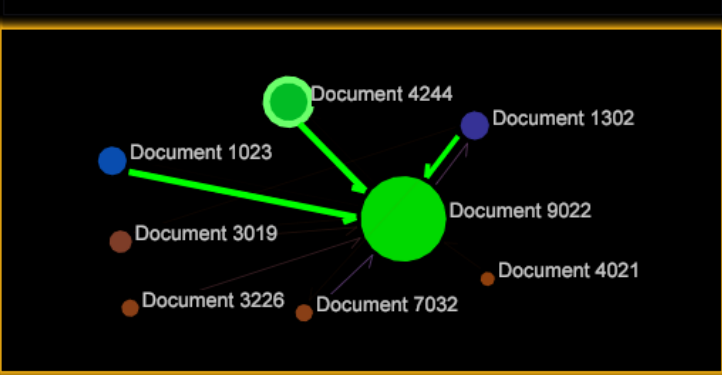
Document Pathing Analysis

Sequence of Documents for each Visitor



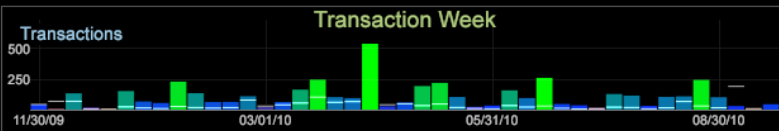
Documents	Document Access	Document Printouts
Document 1302	9,103	320
Document 4021	1,063	20
Document 3226	1,594	13
Document 7032	1,594	13
Document 3019	2,657	1,449

Affinity Analysis

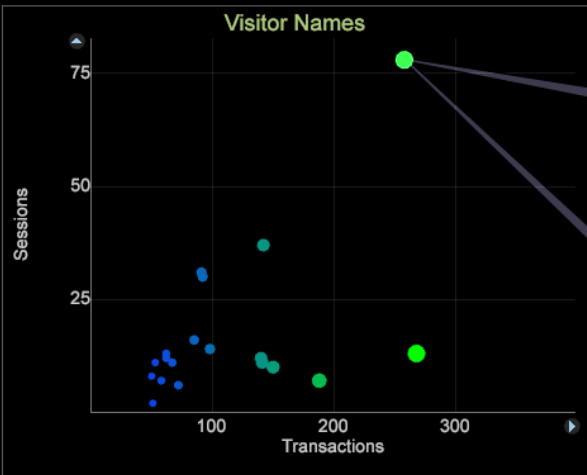


Visitor Activity Analysis

Visitor Names	Sessions	Transactions
Steve Builder	13	268
Steve Higgins	78	258
John Landwehr	7	188
Laurent Duroux	10	150
Marc Eaman	37	142
Barry Graham	11	141
Brendan Nolan	12	140
Mike Denning	14	98
Charles Hanflik	31	91



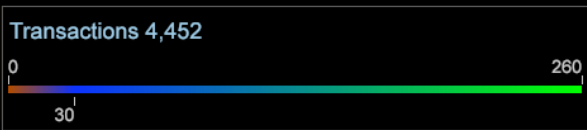
Consumer Bands	Visitors	Sessions	Transactions
Lowest Consumers	1,762	2,032	3,051
Low Consumers	15	221	1,264
Medium Consumers	5	337	3,188



Steve Higgins
New York, NY

Role: Business Analyst
Employee Since: Oct 2006

Accessed Documents	Printouts
Project 003 - (01/05/2008) - draft v3.pdf	2
Project 122 - (03/19/2010) - draft v2.pdf	14
Project 125 - (03/21/2008) - draft v2.pdf	2
Project 192 - (07/12/2009) - draft v3.pdf	2
Project 201 - (04/11/2009) - draft v3.pdf	8
Project 512 - (02/24/2011) - final draft.pdf	70
Project 551 - (07/30/2008) - draft v2.pdf	1
Project 555 - (07/30/2008) - draft v2.pdf	2
Project 651 - (02/10/2010) - draft v1.pdf	3
Project 731 - (06/09/2010) - draft v3.pdf	5
Project 860 - (03/26/2011) - draft v2.pdf	3
Project 928 - (05/03/2009) - draft v4.pdf	2
Project 998 - (12/19/2010) - draft v2.pdf	1



Protecting documents on mobile devices

- Rights management capability in development for mobile devices
- With documents encrypted at document layer, "jailbreaking" a lost/stolen phone does not expose any sensitive information
- Documents can also be revoked, with no further access to decryption key
- Audit log of attempted access is also useful



Summary

- PKI is really good for
 - Digital signatures / certified documents
 - Authentication & authorization
- Standalone PKI is challenging for
 - Asymmetric encryption
- PKI with Rights Management offers
 - Persistent symmetric encryption with PKI authentication and authorization
 - Dynamic control
 - Continuous monitoring

Thank you!

John Landwehr
(202)64ADOBE